Non-instructional Business/
Operations

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. This policy addresses the Elmira City School District's (the District) responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources.

It is the responsibility of the District:

a) to comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;

b) to maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support the District's mission;

c) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure;

d) to address the adherence of its vendors with federal, state and District requirements in its vendor agreements;

e) to train its users to share a measure of responsibility for protecting the District's data and data systems;

f) to identify its required data security and privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and

g) to communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

The policy applies to District employees, and also to independent contractors, interns, student teachers, volunteers ("Users") and third-party contractors who receive or have access to the District's data and/or data systems.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (cont.)

This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of the District and it addresses all information, regardless of the form or format, which is created or used in support of the activities of the District.
This policy shall be published on the District website and notice of its existence shall be provided to all employees and Users.

District Data Privacy and Security Standards

The District will utilize the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program. The Framework is a risk-based approach to managing cybersecurity risk.

The District will protect the privacy of PII by:

a) Ensuring that every use and disclosure of PII by the District benefits students and the District by considering, among other criteria, whether the use and/or disclosure will:

    1. Improve academic achievement;

    2. Empower parents and students with information; and/or

    3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents.

Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

a) The District affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

b) The definition of directory information will be sent home as the annual FERPA Notification.

c) Data protected by law must only be used in accordance with law and regulation and District policies to ensure it is protected from unauthorized use and/or disclosure.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (cont.)

d) No student data shall be shared with third parties without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulation.

e) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with district procedures.

f) It is District policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, the District shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.

g) Contracts with third parties that will receive or have access to personally identifiable information must include a Data Privacy and Security Plan that outlines how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

h) Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under NYS Education Law §2-d and its implementing regulations.

Compliance

Directors, Administrators, and Supervisors are responsible for the compliance of their programs, schools, and offices with this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and Directors, Administrators, and Supervisors will be directed to adopt corrective practices, as applicable.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (cont.)

Oversight of the Data Protection Officer and Data Protection Team

The District will designate a District employee to serve as the District's Data Protection Officer at the annual reorganization meeting each year.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by NYS Education Law §2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

The District has established a Data Protection Team to manage its use of data protected by law. The Data Protection officer and the Data Protection Team will, together with Directors, Administrators, and Supervisors, determine whether a proposed use of personally identifiable information would benefit students and educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed;

Incident Response and Notification

The District will respond to data privacy and security critical incidents in accordance with its **Information Security Breach and Notification Policy.** All breaches of data and/or data systems must be reported to the Data Protection Officer. All breaches of personally identifiable information or sensitive/confidential data must be reported to the State Education Department Chief Privacy Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by NYS Education Law §2-d, or any District sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, the Data Protection Officer will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (cont.)

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The District will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the District has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints with the District about breaches or unauthorized releases of student data and/or teacher or principal data:

a) All complaints must be submitted to the District's Data Protection Officer in writing.

b) Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c) Following the investigation of a submitted complaint, the District will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the District.

d) If the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed the complaint with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, principals, and other District staff.

The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Acceptable Use Policy, Password Policy and other Related District Procedures

a) Users must comply with the **Acceptable Use Policy** in using District resources. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the agency.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (cont.)

b) Users must comply with the **Password Policy**.

c) All remote connections must be made through managed points-of-entry in accordance with the **Acceptable Use Policy**.

Training

All users of District data, data systems and data assets must annually complete the information security and privacy training offered by the District. Information security and privacy training will be made available to all users. Employees must complete the training annually.

Adoption Date: 04/22/2020